

**FILED**

FEB 14 2018

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CLERK U.S. DISTRICT COURT  
WEST. DIST. OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

ALEKSANDRAS PANOVAS

) Criminal No. 18-37  
) [UNDER SEAL]  
) (18 U.S.C. §§ 1030(b),  
) 1349, and 1956(h))  
)

**INDICTMENT**

The grand jury charges:

**INTRODUCTION**

At all times material to this Indictment, unless otherwise alleged:

1) Malicious software (“malware”) is a software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or do other unauthorized action on a computer system. Common examples of malware include viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and others.

2) “Internet Protocol address” or “IP address” is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers’ computers.

3) Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist’s knowledge. Malware that uses keystroke logging often will provide the captured keystrokes to the individual who caused the malware to be

installed or to a place designated by the individual. Through keystroke logging, individuals are able to obtain online banking credentials as soon as the user of the infected computer logs into their account. After obtaining this information, these individuals can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers,<sup>1</sup> to accounts that they control.

4) Web injects introduce (or inject) malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

5) "GozNym" is a multifunction malware package specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of keystroke logging and web injects. GozNym is a hybrid of two previous malware families, Gozi and Nymaim.

6) Financial institutions in the United States first observed fraudulent activity related to GozNym malware in late 2015.

7) GozNym malware was generally distributed through a process known as "phishing", where spam emails were distributed to victims. The emails appeared legitimate and

---

<sup>1</sup> Electronic funds transfers ("EFT") are the exchange and transfer of money through computer-based systems using the Internet. ACH payments allow the electronic transferring of funds from one bank account to another bank account within the ACH network without any paper money changing hands. The ACH network is a network of participating depository financial institutions across the United States, and the network provides for interbank clearing of electronic payments. Because ACH payments require the network to clear the transaction, the funds are not immediately available. Wire transfers also allow electronic transferring of funds from one bank account to another bank account without any paper money changing hands; however, unlike ACH payments, wire transferred funds are immediately available.

were carefully crafted to entice the victim to click on a hyperlink or to open an attached file. In the event a user clicked on a hyperlink, the user was then usually redirected to an exploit kit, which was a web based software program that scans the victim's computer and operating systems for vulnerabilities and upon discovering one, forced the download of a malicious file upon the victim. In the event the victim opened an attached file, he was then directly infected either by the GozNym malware, or by a loader program, which then downloaded the GozNym payload without the victim's consent or knowledge.

8) GozNym malware was used by members of a criminal organization to infect victims' computers for the purpose of capturing the victims' online banking credentials. Using those captured credentials, members of the organization gained unauthorized access to victims' online bank accounts and caused, or attempted to cause, electronic funds transfers from the victims' bank accounts into bank accounts controlled by the defendant, ALEKSANDRAS PANOVAS, and other members of the organization.

9) Members of the GozNym criminal organization were members of the criminal conspiracies (collectively "GozNym conspiracy") charged in Counts One, Two, and Three, of this Indictment.

10) GozNym, like most modern malware families, was specifically crafted to defeat antivirus and other protective measures employed by victims.

11) GozNym malware has infected thousands of victim computers worldwide, including in the Western District of Pennsylvania.

12) GozNym malware infections have resulted in tens of millions of dollars in losses and attempted losses.

13) An "electronic funds transfer" (EFT) is the electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, via computer-based systems, without the direct intervention of bank staff. Types of

electronic funds transfers include automated clearing house (ACH) transactions, wire transfers, and SWIFT payments.

14) A “SWIFT payment” is a type of international transfer of funds sent via the SWIFT international payment network. SWIFT (Society for Worldwide Interbank Financial Telecommunication) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure and standardized environment.

15) A “drop account” is a bank account fraudulently created for the purpose of receiving stolen funds from victim bank accounts through electronic funds transfers.

16) A “drop master” is an individual who controls one or more “drop accounts.” A “drop master” provides other cybercriminals with access to “drop accounts” for the purpose of receiving stolen funds. Using his associates, the “drop master” oversees the process of getting the stolen funds out of the “drop account” and back to the members of the conspiracy.

17) First National Bank of Pennsylvania (FNB) was a financial institution insured by the Federal Deposit Insurance Corporation. FNB was headquartered in Pittsburgh, Pennsylvania, in the Western District of Pennsylvania. It offered online banking services, including the means to conduct electronic funds transfers, through computer servers located in the Western District of Pennsylvania.

18) PNC Bank (PNC) was a financial institution insured by the Federal Deposit Insurance Corporation. PNC was headquartered in Pittsburgh, Pennsylvania, in the Western District of Pennsylvania. It offered online banking services, including the means to conduct electronic funds transfers, through computer servers located in the Western District of Pennsylvania.

19) Bridge Bank, a division of Western Alliance Bank, was a financial institution insured by the Federal Deposit Insurance Corporation. Bridge Bank was headquartered

in San Jose, California. It offered online banking services, including the means to conduct electronic funds transfers.

20) Wells Fargo Bank (Wells Fargo) was a financial institution insured by the Federal Deposit Insurance Corporation. Wells Fargo was headquartered in San Francisco, California. It offered online banking services, including the means to conduct electronic funds transfers.

21) Protech Asphalt Maintenance, Inc. (Protech) was an asphalt and paving business located in New Castle, Pennsylvania, in the Western District of Pennsylvania.

22) Nord-Lock, Inc. (Nord-Lock) was a bolt manufacturing company located in Carnegie, Pennsylvania, in the Western District of Pennsylvania.

23) Horizon Solar Power Corporation (Horizon) was a designer and installer of residential and commercial solar power systems, located in Hemet, California.

24) B.G., an individual whose identity is known to the grand jury, was the beneficiary of a trust account at Wells Fargo in San Francisco, California.

25) The defendant, ALEKSANDRAS PANOVAS, was a Lithuanian National residing in the United Kingdom. PANOVAS' primary role in the conspiracies charged in Counts One, Two and Three of this Indictment, was that of a "drop master." In that capacity, ALEKSANDRAS PANOVAS provided members of the conspiracy with access to bank accounts, also known as "drop accounts," controlled by ALEKSANDRAS PANOVAS and into which ALEKSANDRAS PANOVAS and his co-conspirators transmitted, and attempted to transmit, electronic funds transfers containing funds stolen from victims' online bank accounts.

MANNER AND MEANS OF THE CHARGED CONSPIRACIES

26) Members of the conspiracy, known and unknown to the grand jury, sent phishing emails through the Internet that falsely represented themselves to be legitimate emails from legitimate companies, associations, and organizations.

27) Members of the conspiracy, known and unknown to the grand jury, created the phishing emails to fraudulently induce recipients to click on a hyperlink or attachment that falsely represented itself to be a legitimate link or attachment containing business or personal information, typically an attachment designed to appear as a legitimate business invoice, when in truth and fact, it installed malware on the email recipients' computers without the email recipients' consent or knowledge.

28) Members of the conspiracy, known and unknown to the grand jury, without authorization, installed and caused the installation of the GozNym malware on Internet-connected victim computers.

29) Members of the conspiracy, known and unknown to the grand jury, used the GozNym malware on infected computers to capture the user's confidential personal and financial information, including online banking credentials, by keystroke logging or by hijacking the computer session and presenting a web inject, i.e., fake online banking webpages.

30) Members of the conspiracy, known and unknown to the grand jury, used the captured banking credentials without authorization to falsely represent to banks that conspirators were victims or employees of victims who had authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

31) Members of the conspiracy, known and unknown to the grand jury, used the captured banking credentials to gain unauthorized access to victims' online bank accounts and caused, and attempted to cause, banks to make unauthorized wire transfers, ACH payments, or

other electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the account holders.

32) The defendant, ALEKSANDRAS PANOVAS, provided members of the conspiracy with access to bank accounts, also known as "drop accounts," controlled by the defendant, ALEKSANDRAS PANOVAS, for the purpose of receiving and laundering stolen funds from victims' online bank accounts.

33) The defendant, ALEKSANDRAS PANOVAS, utilized associates in Hong Kong, including bank employees with access to the SWIFT network, to receive and launder the stolen funds and to further distribute the funds to designated bank accounts controlled by members of the conspiracy.

34) Members of the conspiracy, known and unknown to the grand jury, during the initial stages of developing GozNym malware, created an administrative panel to assist them in conducting the scheme. The administrative panel was simply an interface hosted on a server that was configured to allow the co-conspirators to see the victims that had been infected with GozNym malware and access their confidential banking information. The earliest of these administrative panels used the domain fokentoken.com and was hosted at IP address 204.155.30.87. Subsequent panels were hosted at IP address 204.155.31.133, and thereafter at IP address 204.155.30.8.

#### OVERT ACTS

35) In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendant, ALEKSANDRAS PANOVAS, and co-conspirators both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

36) On or about November 15, 2015, the defendant ALEKSANDRAS PANOVAS, using a secure instant messaging communication platform, provided a conspiracy

member known to the grand jury with a detailed explanation of the “cash out” services the defendant could provide to members of the conspiracy.

37) On or about December 4, 2015, the defendant, ALEKSANDRAS PANOVAS, using a secure instant messaging communication platform, discussed with a conspiracy member known to the grand jury the percentage split of the stolen funds to be received by members of the conspiracy, including a conspiracy leader known to the grand jury.

38) On or about December 2, 2015, the defendant, ALEKSANDRAS PANOVAS, provided a conspiracy leader known to the grand jury with access to the following Hong Kong bank account for the purpose of receiving up to \$500,000 in electronic funds transfers from U.S. victims’ bank accounts: Nanyang Commercial Bank Limited, 151 Des Voeux Road Central, Hong Kong, account number XXXXXXXXXXXX3299 in the name S.C.K., SWIFT Code XXXXXKHH.

39) On or about December 2, 2015, members of the conspiracy, known and unknown to the grand jury, sent to an employee of Horizon Solar Power Corporation (Horizon) a phishing email which fraudulently induced the employee to click on a link or an attachment falsely represented to be legitimate, and in doing so caused the Horizon employee to unwittingly install malware on Horizon’s computer.

40) On or about December 2, 2015, members of the conspiracy, known and unknown to the grand jury, fraudulently caused and attempted to cause the electronic funds transfer of \$380,000.00 from Horizon’s account at Bridge Bank to Nanyang Commercial Bank Limited, 151 Des Voeux Road Central, Hong Kong, account number XXXXXXXXXXXX3299 in the name S.C.K., SWIFT Code XXXXXKHH, a drop account controlled by the defendant, ALEKSANDRAS PANOVAS.

41) On or about December 4, 2015, the defendant, ALEKSANDRAS PANOVAS, provided a conspiracy member known to the grand jury with access to the following



Hong Kong bank account for the purpose of receiving up to \$500,000 in electronic funds transfers from U.S. victims' bank accounts: Nanyang Commercial Bank Limited, 151 Des Voeux Road Central, Hong Kong, account number XXXXXXXXXXX3299 in the name S.C.K., SWIFT Code XXXXXKHH.

42) On or about December 28, 2015, members of the conspiracy, known and unknown to the grand jury, fraudulently caused and attempted to cause the electronic funds transfer of \$326,700.00 from B.G.'s trust account at Wells Fargo Bank to Nanyang Commercial Bank Limited, 151 Des Voeux Road Central, Hong Kong, account number XXXXXXXXXXX3299 in the name S.C.K., SWIFT Code XXXXXKHH, a drop account controlled by the defendant, ALEKSANDRAS PANOVAS.

43) On or about February 18, 2016, members of the conspiracy, known and unknown to the grand jury, sent to an employee of Protech Asphalt Maintenance, Inc. (Protech), located in the Western District of Pennsylvania, a phishing email which fraudulently induced the employee to click on a link or an attachment falsely represented to be legitimate, and in doing so caused the Protech employee to unwittingly install GozNym malware on Protech's computer.

44) On or about February 24, 2016, members of the conspiracy, known and unknown to the grand jury, used the banking credentials of Protech employees acquired through GozNym malware to gain unauthorized access to Protech's account at First National Bank and fraudulently caused and attempted to cause the following three electronic funds transfers in the amounts specified below totaling \$121,132.08, from Protech's account to the accounts specified below:

- a) \$74,287.80 to an account in the name of DCSH at Bank of America;
- b) \$39,856.88 to an account in the name of DCSH at Bank of America;  
and
- c) \$6,987.40 to an account in the name of S.W. at Bank of America.

45) On or about April 7, 2016, members of the conspiracy, known and unknown to the grand jury, sent to an employee of Nord-Lock, Inc. (Nord-Lock), located in the Western District of Pennsylvania, a phishing email which fraudulently induced the employee to click on a link or an attachment falsely represented to be legitimate, and in doing so caused the Nord-Lock employee to unwittingly install GozNym malware on Nord-Lock's computer.

46) On or about April 11, 2016, members of the conspiracy, known and unknown to the grand jury, fraudulently caused and attempted to cause the electronic funds transfer of \$387,500.00 from Nord-Lock's account at PNC Bank, in the Western District of Pennsylvania, to bank account number XXXXXXXXXXXXXXXXXXXX7438 in the name of A.A. EOOD at D Commerce Bank AD, Sofia, Bulgaria.

47) On or about April 12, 2016, in the Western District of Pennsylvania, members of the conspiracy, known and unknown to the grand jury, fraudulently caused and attempted to cause the following four electronic funds transfers in the amounts specified below totaling \$122,000.00, from Protech's account at First National Bank to the accounts specified below:

- a) \$93,200.00 to Bank Account Number: XXXXXX7793 in the name of N.M.J. at Bank Midwest, Olathe, Kansas;
- b) \$9,600.00 to Bank Account Number: XXXXXXXX2352 in the name of J.P. at GoBank in Provo, Utah;
- c) \$9,600.00 to Bank Account Number: XXXXXX2862 in the name of K.H. at Wells Fargo Bank in Brandon, Florida; and
- d) \$9,600.00 to Bank Account Number: XXXXXX3770 in the name of M.D.L.R. at Chase Bank in Palm Harbor, Florida.

**COUNT ONE**  
**(Computer Fraud Conspiracy)**

The grand jury further charges:

48) The allegations contained in Paragraphs 1 through 47 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

**THE CONSPIRACY AND ITS OBJECTS**

49) From in and around November 2015, and continuing thereafter until on or about November 30, 2016, in the Western District of Pennsylvania and elsewhere, the defendant, ALEKSANDRAS PANOVAS, intentionally and knowingly did conspire, combine, and agree with other persons known and unknown to the grand jury, to commit computer fraud, and to aid and abet the same, contrary to the provisions of Title 18, United States Code, Section 1030(a)(2), to wit:

the defendant, ALEKSANDRAS PANOVAS, and others known and unknown to the grand jury, did intentionally access a computer, without authorization, and thereby obtain or attempt to obtain information in a financial record of a financial institution for the purpose of private financial gain, contrary to the provisions of Title 18, United States Code, Sections 1030(a)(2)(A) and 1030(c)(2)(B)(i).

50) It was further a part of the conspiracy that members of the conspiracy, known and unknown to the grand jury, used stolen banking credentials acquired through GozNym malware infections to gain unauthorized access to victims' online bank accounts to obtain financial information used in furtherance of unauthorized electronic funds transfers.

51) It was further a part of the conspiracy that the defendant, ALEKSANDRAS PANOVAS, provided members of the conspiracy with access to bank accounts, also known as "drop accounts," designated to receive stolen funds, in the form of electronic funds transfers, from victims' online bank accounts.

In violation of Title 18, United States Code, Sections 1030(b).

**COUNT TWO**  
**(Bank Fraud Conspiracy)**

The grand jury further charges:

52) The allegations contained in Paragraphs 1 through 47 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

**THE CONSPIRACY AND ITS OBJECTS**

53) From in and around November 2015, and continuing thereafter until on or about November 30, 2016, in the Western District of Pennsylvania and elsewhere, the defendant, ALEKSANDRAS PANOVAS, knowingly and willfully did conspire, combine, and agree with other persons known and unknown to the grand jury, to commit an offense against the United States, that is, bank fraud, contrary to the provisions of Title 18, United States Code, Section 1344, to wit:

the defendant, ALEKSANDRAS PANOVAS, and others known and unknown to the grand jury, did execute, and attempt to execute, a scheme and artifice to defraud financial institutions and to obtain moneys and funds owned by and under the custody and control of said financial institutions by means of material false and fraudulent pretenses, representations and promises, well knowing that the pretenses, representations and promises would be and were false and fraudulent.

54) It was a part of the conspiracy that members of the conspiracy, known and unknown to the grand jury, used the victims' captured banking credentials without authorization to falsely represent to banks that the defendant and co-conspirators were victims or employees of victims who had authorization to access the victims' bank accounts and to make unauthorized electronic funds transfers from the victims' bank accounts.

55) It was further a part of the conspiracy that the defendant, ALEKSANDRAS PANOVAS, and others known and unknown to the grand jury, did knowingly execute, and attempt

to execute, the foregoing scheme and artifice by causing, and attempting to cause, the transfer of stolen funds from the victims' bank accounts into bank accounts, also known as "drop accounts," provided and controlled by the defendant, ALEKSANDRAS PANOVAS.

In violation of Title 18, United States Code, Sections 1349.

**COUNT THREE**  
**(Money Laundering Conspiracy)**

The grand jury further charges:

56) The allegations contained in Paragraphs 1 through 47 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

**THE CONSPIRACY AND ITS OBJECTS**

57) From in and around November 2015, and continuing thereafter until on or about November 30, 2016, in the Western District of Pennsylvania and elsewhere, the defendant, ALEKSANDRAS PANOVAS, and others known and unknown to the grand jury, intentionally and knowingly did combine, conspire, and agree together and with each other to knowingly commit money laundering offenses, that is:

a. To knowingly conduct and attempt to conduct financial transactions involving property representing the proceeds of specified unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, knowing that the transactions were designed, in whole or in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of the specified unlawful activity, contrary to the provisions of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

b. To knowingly transport, transmit, transfer, and attempt to transport, transmit, and transfer funds from a place in the United States to a place outside the United States, knowing that the funds involved in the transportation, transmission, and transfer represent the proceeds of unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, and knowing that such transportation, transmission, and transfer is designed, in whole or in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of the specified unlawful activity, contrary to the provisions of Title 18, United States Code, Section 1956(a)(2)(B)(i);

to wit, the defendant, ALEKSANDRAS PANOVAS, and others known and unknown to the grand jury, did conduct and attempt to conduct unauthorized electronic funds transfers from victims' online bank accounts into bank accounts controlled by ALEKSANDRAS PANOVAS but in the names of third parties, for the purpose of concealing and disguising the nature, location, source, ownership and control of said proceeds.

In violation of Title 18, United States Code, Section 1956(h).

**FORFEITURE ALLEGATION**

58) The allegations contained in Counts One through Three of this Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 1030(i), and Title 28, United States Code, Section 2461(c).

59) Upon conviction of the computer fraud conspiracy offense alleged in Count One of this Indictment, the defendant, ALEKSANDRAS PANOVAS, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B), and 1030(i), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense, and any interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

60) Upon conviction of the bank fraud conspiracy offense in Count Two of this Indictment, the defendant, ALEKSANDRAS PANOVAS, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and 28 United States Code, Section 2461(c), any property, real or personal, which constitutes, and is derived from, proceeds traceable, directly and indirectly, to such violations. The property to be forfeited includes, but is not limited to, a money judgment for a sum of money equal to the proceeds obtained as a result of the offenses.

61) Upon conviction of the money laundering conspiracy offense in Count Three of this Indictment, the defendant, ALEKSANDRAS PANOVAS, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in the offense, or any property traceable to such property.

62) If through any acts or omission by the defendant, ALEKSANDRAS PANOVAS, any or all of the property described in paragraphs 59 through 61 above (hereinafter the "Subject Properties"):



- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without

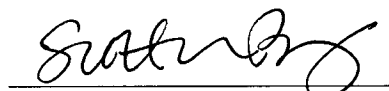
difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i), and Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 982(b) and 1030(i), Title 21, United States Code, Section 853, and Title 28, United States Code, Section 2461(c).

A True Bill,

  
FOREPERSON

  
SCOTT W. BRADY  
United States Attorney  
PA ID No. 88352